

A person is silhouetted against a bright sunset, standing on a dark, rocky mountain peak. The person is looking out over a vast, undulating sea of white and orange-tinted clouds that stretch to the horizon. The sun is a bright, glowing orb in the upper center of the frame, casting a warm, golden light across the entire scene. The sky above the clouds is a pale, hazy yellow.

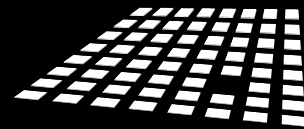
Standing on the Clouds

A journey in Private Cloud Security
Claudio Criscione - @paradoxengine
SyScan 10

/me



Claudio Criscione



VIRTUALIZATION.INFO

There are a lot of clouds



very Fluffy Clouds...



...And less fluffy

A Taxonomy of clouds

Cloud by the book - NIST

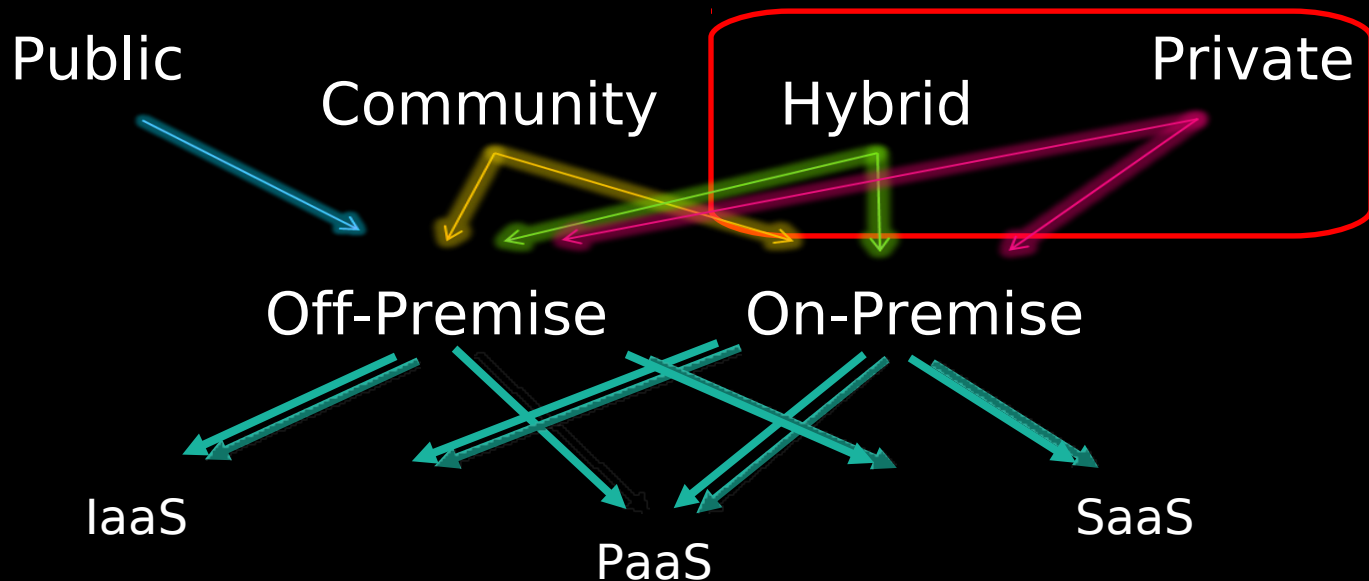
On-demand self-service

Broad network access

Resource pooling

Rapid elasticity

Measured Service



Who plays the game?

XEN – XenCloud

VMware [And the VMware Express players]

Ubuntu – Eucalyptus

Red Hat – DeltaCloud, RHVM

Amazon – Virtual Private Cloud

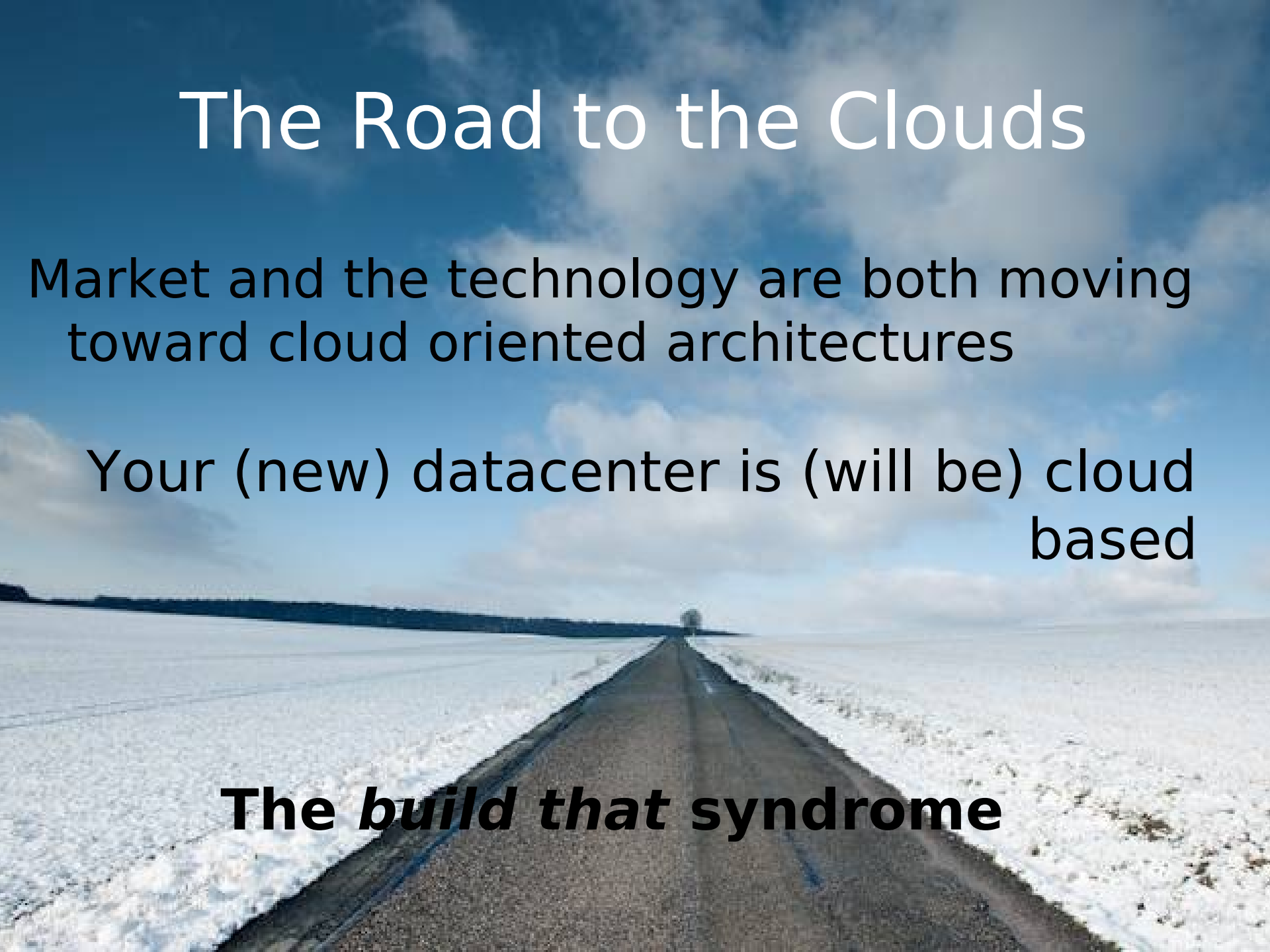
...and many others

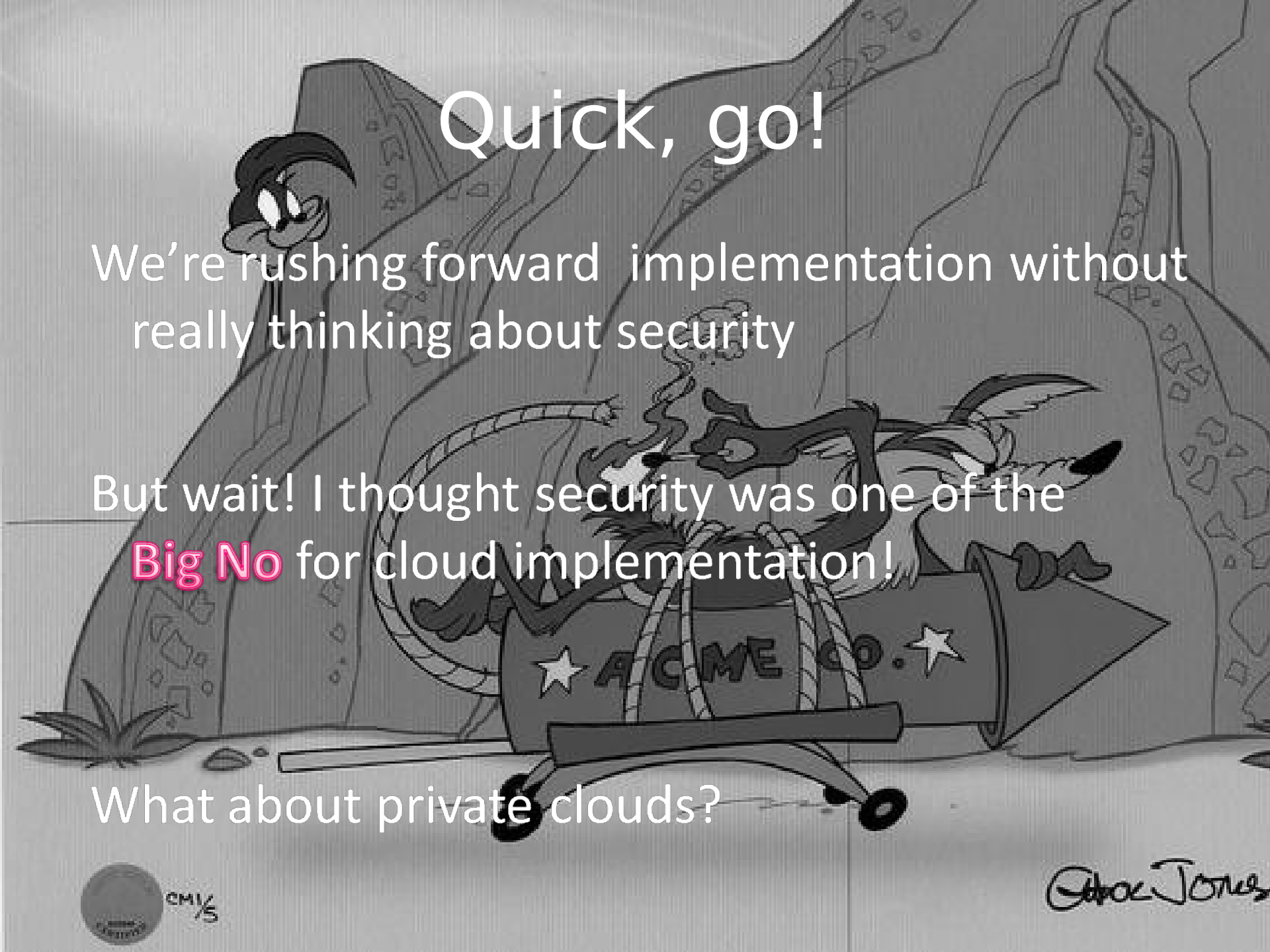
The Road to the Clouds

Market and the technology are both moving toward cloud oriented architectures

Your (new) datacenter is (will be) cloud based

The *build that* syndrome





Quick, go!

We're rushing forward implementation without really thinking about security

But wait! I thought security was one of the **Big No** for cloud implementation!

What about private clouds?



Steve Jones

A trojan horse

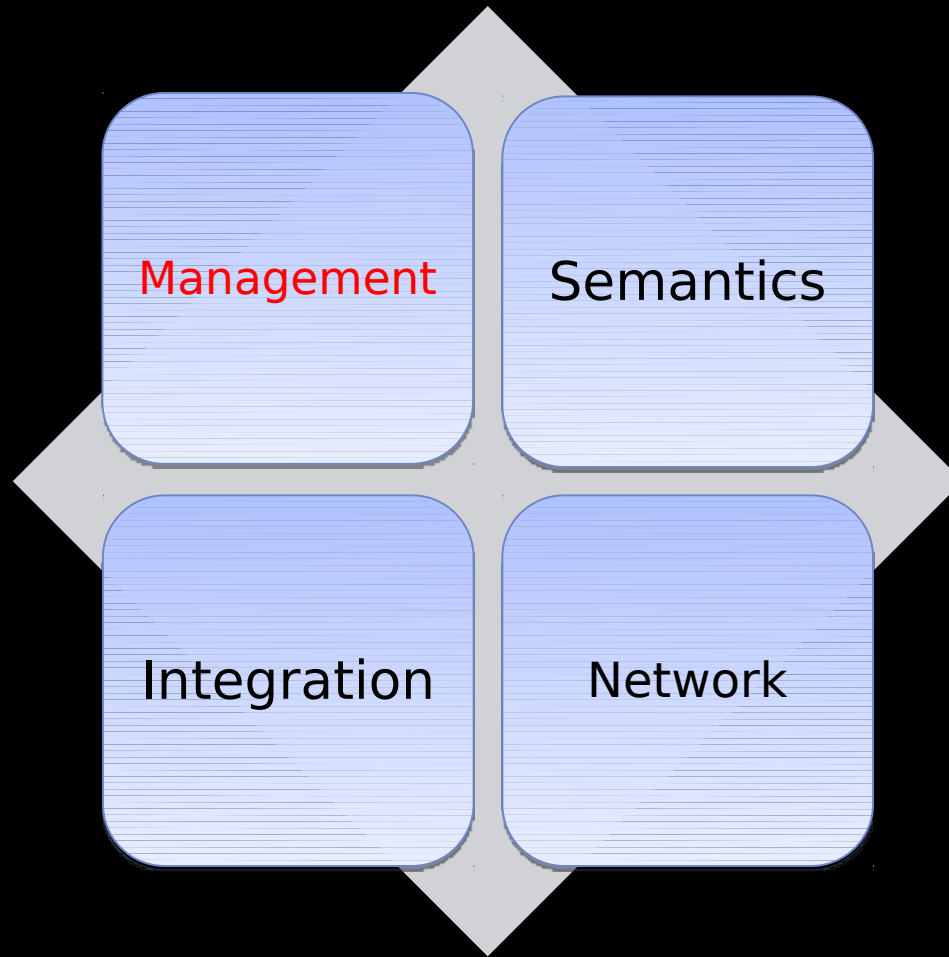
Private Clouds are the “Trojan horse”
of the Cloud Industry

It's just like standard virtualization!

In the meantime, you get used
to those small deltas...



Security Deltas



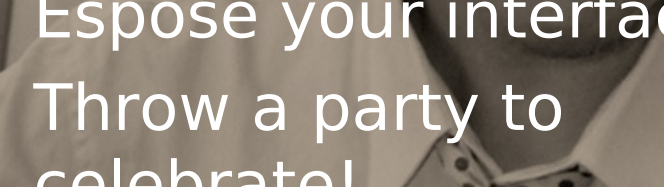
Management

The “Old Virtualization” Way

-
- A person's arm is visible on the right side, holding a piece of chalk and writing on a dark chalkboard. The chalkboard is covered with handwritten text in white chalk, including various network protocols and concepts such as "IP", "TCP", "UDP", "DNS", "HTTP", "FTP", "SMTP", "POP3", "IMAP", "SSH", "Telnet", "RDP", "VNC", "VPN", "SSL/TLS", "DHCP", "NTP", "SNMP", "BGP", "OSPF", "EIGRP", "IS-IS", "MPLS", "SD-WAN", "Network Security", "Firewall", "IDS/IPS", "SIEM", "Incident Response", "Penetration Testing", "Ethical Hacking", "Social Engineering", "Phishing", "Malware", "Ransomware", "Data Breach", "Cybersecurity", "Information Security", "Risk Management", "Compliance", "GDPR", "HIPAA", "PCI-DSS", "ISO 27001", "NIST", "CIS", "MITRE ATT&CK", "OWASP Top 10", "CVE", "CVE-2021-44228", "Log4j", "Heartbleed", "Shellshock", "Buffer Overflow", "SQL Injection", "XSS", "CSRF", "Cross-Site Scripting", "Man-in-the-Middle", "Denial of Service", "Zero-Day", "Exploit", "Vulnerability", "Patch", "Update", "Security Audit", "Vulnerability Assessment", "Penetration Test", "Red Team", "Blue Team", "Purple Team", "Cyber Range", "Training", "Certification", "CompTIA Network+", "Cisco CCNA", "Microsoft Certified Solutions Provider", "AWS Certified Solutions Architect", "Google Cloud Professional Network Engineer", "Oracle Certified Professional", "VMware VCP", "Palo Alto Networks Certified Network Security Administrator", "Juniper Networks Certified Network Associate", "Huawei HCNP", "H3C H13", "Fortinet NSE4", "Check Point Certified Expert", "Cisco Certified Internetwork Specialist", "Cisco Certified Network Professional", "Cisco Certified Design Professional", "Cisco Certified Design Specialist", "Cisco Certified Implementation Specialist", "Cisco Certified Support Specialist", "Cisco Certified Technical Assistant", "Cisco Certified Entry-Level Technician", "Cisco Certified End User", "Cisco Certified Partner", "Cisco Certified Reseller", "Cisco Certified Distributor", "Cisco Certified Integrator", "Cisco Certified Managed Service Provider", "Cisco Certified Consulting Partner", "Cisco Certified Training Partner", "Cisco Certified Marketing Partner", "Cisco Certified Sales Partner", "Cisco Certified Business Partner", "Cisco Certified Global Partner", "Cisco Certified International Partner", "Cisco Certified Local Partner", "Cisco Certified Regional Partner", "Cisco Certified Country Partner", "Cisco Certified Multi-Country Partner", "Cisco Certified Multi-Region Partner", "Cisco Certified Multi-Sector Partner", "Cisco Certified Multi-Industry Partner", "Cisco Certified Multi-Segment Partner", "Cisco Certified Multi-Channel Partner", "Cisco Certified Multi-Touchpoint Partner", "Cisco Certified Multi-Device Partner", "Cisco Certified Multi-Platform Partner", "Cisco Certified Multi-Ecosystem Partner", "Cisco Certified Multi-Environment Partner", "Cisco Certified Multi-Scenario Partner", "Cisco Certified Multi-Use Case Partner", "Cisco Certified Multi-Problem Partner", "Cisco Certified Multi-Solution Partner", "Cisco Certified Multi-Benefit Partner", "Cisco Certified Multi-Value Partner", "Cisco Certified Multi-Experience Partner", "Cisco Certified Multi-Journey Partner", "Cisco Certified Multi-Outcome Partner", "Cisco Certified Multi-Mission Partner", "Cisco Certified Multi-Purpose Partner", "Cisco Certified Multi-Function Partner", "Cisco Certified Multi-Feature Partner", "Cisco Certified Multi-Service Partner", "Cisco Certified Multi-Application Partner", "Cisco Certified Multi-System Partner", "Cisco Certified Multi-Infrastructure Partner", "Cisco Certified Multi-Network Partner", "Cisco Certified Multi-Cloud Partner", "Cisco Certified Multi-On-Premise Partner", "Cisco Certified Multi-Hybrid Partner", "Cisco Certified Multi-Edge Partner", "Cisco Certified Multi-Core Partner", "Cisco Certified Multi-Brain Partner", "Cisco Certified Multi-Sense Partner", "Cisco Certified Multi-Act Partner", "Cisco Certified Multi-Think Partner", "Cisco Certified Multi-Feel Partner", "Cisco Certified Multi-Taste Partner", "Cisco Certified Multi-Smell Partner", "Cisco Certified Multi-Touch Partner", "Cisco Certified Multi-Move Partner", "Cisco Certified Multi-Speak Partner", "Cisco Certified Multi-Interact Partner", "Cisco Certified Multi-Engage Partner", "Cisco Certified Multi-Connect Partner", "Cisco Certified Multi-Share Partner", "Cisco Certified Multi-Collaborate Partner", "Cisco Certified Multi-Work Partner", "Cisco Certified Multi-Learn Partner", "Cisco Certified Multi-Grow Partner", "Cisco Certified Multi-Innovate Partner", "Cisco Certified Multi-Transform Partner", "Cisco Certified Multi-Improve Partner", "Cisco Certified Multi-Optimize Partner", "Cisco Certified Multi-Maximize Partner", "Cisco Certified Multi-Amplify Partner", "Cisco Certified Multi-Magnify Partner", "Cisco Certified Multi-Expand Partner", "Cisco Certified Multi-Stretch Partner", "Cisco Certified Multi-Extend Partner", "Cisco Certified Multi-Reach Partner", "Cisco Certified Multi-Access Partner", "Cisco Certified Multi-Reachable Partner", "Cisco Certified Multi-Accessible Partner", "Cisco Certified Multi-Usable Partner", "Cisco Certified Multi-Operable Partner", "Cisco Certified Multi-Manageable Partner", "Cisco Certified Multi-Maintainable Partner", "Cisco Certified Multi-Upgradeable Partner", "Cisco Certified Multi-Replaceable Partner", "Cisco Certified Multi-Disposable Partner", "Cisco Certified Multi-Reusable Partner", "Cisco Certified Multi-Restorable Partner", "Cisco Certified Multi-Recoverable Partner", "Cisco Certified Multi-Resilient Partner", "Cisco Certified Multi-Tolerant Partner", "Cisco Certified Multi-Adaptable Partner", "Cisco Certified Multi-Flexible Partner", "Cisco Certified Multi-Versatile Partner", "Cisco Certified Multi-Multifunctional Partner", "Cisco Certified Multi-Multi-Purpose Partner", "Cisco Certified Multi-Multi-Function Partner", "Cisco Certified Multi-Multi-Feature Partner", "Cisco Certified Multi-Multi-Service Partner", "Cisco Certified Multi-Multi-Application Partner", "Cisco Certified Multi-Multi-System Partner", "Cisco Certified Multi-Multi-Infrastructure Partner", "Cisco Certified Multi-Multi-Network Partner", "Cisco Certified Multi-Multi-Cloud Partner", "Cisco Certified Multi-Multi-On-Premise Partner", "Cisco Certified Multi-Multi-Hybrid Partner", "Cisco Certified Multi-Multi-Edge Partner", "Cisco Certified Multi-Multi-Core Partner", "Cisco Certified Multi-Multi-Brain Partner", "Cisco Certified Multi-Multi-Sense Partner", "Cisco Certified Multi-Multi-Act Partner", "Cisco Certified Multi-Multi-Think Partner", "Cisco Certified Multi-Multi-Feel Partner", "Cisco Certified Multi-Multi-Taste Partner", "Cisco Certified Multi-Multi-Smell Partner", "Cisco Certified Multi-Multi-Touch Partner", "Cisco Certified Multi-Multi-Move Partner", "Cisco Certified Multi-Multi-Speak Partner", "Cisco Certified Multi-Multi-Interact Partner", "Cisco Certified Multi-Multi-Engage Partner", "Cisco Certified Multi-Multi-Connect Partner", "Cisco Certified Multi-Multi-Share Partner", "Cisco Certified Multi-Multi-Collaborate Partner", "Cisco Certified Multi-Multi-Work Partner", "Cisco Certified Multi-Multi-Learn Partner", "Cisco Certified Multi-Multi-Grow Partner", "Cisco Certified Multi-Multi-Innovate Partner", "Cisco Certified Multi-Multi-Transform Partner", "Cisco Certified Multi-Multi-Improve Partner", "Cisco Certified Multi-Multi-Optimize Partner", "Cisco Certified Multi-Multi-Maximize Partner", "Cisco Certified Multi-Multi-Amplify Partner", "Cisco Certified Multi-Multi-Magnify Partner", "Cisco Certified Multi-Multi-Expand Partner", "Cisco Certified Multi-Multi-Stretch Partner", "Cisco Certified Multi-Multi-Extend Partner", "Cisco Certified Multi-Multi-Reach Partner", "Cisco Certified Multi-Multi-Access Partner", "Cisco Certified Multi-Multi-Reachable Partner", "Cisco Certified Multi-Multi-Accessible Partner", "Cisco Certified Multi-Multi-Usable Partner", "Cisco Certified Multi-Multi-Operable Partner", "Cisco Certified Multi-Multi-Manageable Partner", "Cisco Certified Multi-Multi-Maintainable Partner", "Cisco Certified Multi-Multi-Upgradeable Partner", "Cisco Certified Multi-Multi-Replaceable Partner", "Cisco Certified Multi-Multi-Disposable Partner", "Cisco Certified Multi-Multi-Reusable Partner", "Cisco Certified Multi-Multi-Restorable Partner", "Cisco Certified Multi-Multi-Recoverable Partner", "Cisco Certified Multi-Multi-Resilient Partner", "Cisco Certified Multi-Multi-Tolerant Partner", "Cisco Certified Multi-Multi-Adaptable Partner", "Cisco Certified Multi-Multi-Flexible Partner", "Cisco Certified Multi-Multi-Versatile Partner", "Cisco Certified Multi-Multi-Multifunctional Partner", "Cisco Certified Multi-Multi-Multi-Purpose Partner", "Cisco Certified Multi-Multi-Multi-Function Partner", "Cisco Certified Multi-Multi-Multi-Feature Partner", "Cisco Certified Multi-Multi-Multi-Service Partner", "Cisco Certified Multi-Multi-Multi-Application Partner", "Cisco Certified Multi-Multi-Multi-System Partner", "Cisco Certified Multi-Multi-Multi-Infrastructure Partner", "Cisco Certified Multi-Multi-Multi-Network Partner", "Cisco Certified Multi-Multi-Multi-Cloud Partner", "Cisco Certified Multi-Multi-Multi-On-Premise Partner", "Cisco Certified Multi-Multi-Multi-Hybrid Partner", "Cisco Certified Multi-Multi-Multi-Edge Partner", "Cisco Certified Multi-Multi-Multi-Core Partner", "Cisco Certified Multi-Multi-Multi-Brain Partner", "Cisco Certified Multi-Multi-Multi-Sense Partner", "Cisco Certified Multi-Multi-Multi-Act Partner", "Cisco Certified Multi-Multi-Multi-Think Partner", "Cisco Certified Multi-Multi-Multi-Feel Partner", "Cisco Certified Multi-Multi-Multi-Taste Partner", "Cisco Certified Multi-Multi-Multi-Smell Partner", "Cisco Certified Multi-Multi-Multi-Touch Partner", "Cisco Certified Multi-Multi-Multi-Move Partner", "Cisco Certified Multi-Multi-Multi-Speak Partner", "Cisco Certified Multi-Multi-Multi-Interact Partner", "Cisco Certified Multi-Multi-Multi-Engage Partner", "Cisco Certified Multi-Multi-Multi-Connect Partner", "Cisco Certified Multi-Multi-Multi-Share Partner", "Cisco Certified Multi-Multi-Multi-Collaborate Partner", "Cisco Certified Multi-Multi-Multi-Work Partner", "Cisco Certified Multi-Multi-Multi-Learn Partner", "Cisco Certified Multi-Multi-Multi-Grow Partner", "Cisco Certified Multi-Multi-Multi-Innovate Partner", "Cisco Certified Multi-Multi-Multi-Transform Partner", "Cisco Certified Multi-Multi-Multi-Improve Partner", "Cisco Certified Multi-Multi-Multi-Optimize Partner", "Cisco Certified Multi-Multi-Multi-Maximize Partner", "Cisco Certified Multi-Multi-Multi-Amplify Partner", "Cisco Certified Multi-Multi-Multi-Magnify Partner", "Cisco Certified Multi-Multi-Multi-Expand Partner", "Cisco Certified Multi-Multi-Multi-Stretch Partner", "Cisco Certified Multi-Multi-Multi-Extend Partner", "Cisco Certified Multi-Multi-Multi-Reach Partner", "Cisco Certified Multi-Multi-Multi-Access Partner", "Cisco Certified Multi-Multi-Multi-Reachable Partner", "Cisco Certified Multi-Multi-Multi-Accessible Partner", "Cisco Certified Multi-Multi-Multi-Usable Partner", "Cisco Certified Multi-Multi-Multi-Operable Partner", "Cisco Certified Multi-Multi-Multi-Manageable Partner", "Cisco Certified Multi-Multi-Multi-Maintainable Partner", "Cisco Certified Multi-Multi-Multi-Upgradeable Partner", "Cisco Certified Multi-Multi-Multi-Replaceable Partner", "Cisco Certified Multi-Multi-Multi-Disposable Partner", "Cisco Certified Multi-Multi-Multi-Reusable Partner", "Cisco Certified Multi-Multi-Multi-Restorable Partner", "Cisco Certified Multi-Multi-Multi-Recoverable Partner", "Cisco Certified Multi-Multi-Multi-Resilient Partner", "Cisco Certified Multi-Multi-Multi-Tolerant Partner", "Cisco Certified Multi-Multi-Multi-Adaptable Partner", "Cisco Certified Multi-Multi-Multi-Flexible Partner", "Cisco Certified Multi-Multi-Multi-Versatile Partner", "Cisco Certified Multi-Multi-Multi-Multifunctional Partner", "Cisco Certified Multi-Multi-Multi-Multi-Purpose Partner", "Cisco Certified Multi-Multi-Multi-Multi-Function Partner", "Cisco Certified Multi-Multi-Multi-Multi-Feature Partner", "Cisco Certified Multi-Multi-Multi-Multi-Service Partner", "Cisco Certified Multi-Multi-Multi-Multi-Application Partner", "Cisco Certified Multi-Multi-Multi-Multi-System Partner", "Cisco Certified Multi-Multi-Multi-Multi-Infrastructure Partner", "Cisco Certified Multi-Multi-Multi-Multi-Network Partner", "Cisco Certified Multi-Multi-Multi-Multi-Cloud Partner", "Cisco Certified Multi-Multi-Multi-Multi-On-Premise Partner", "Cisco Certified Multi-Multi-Multi-Multi-Hybrid Partner", "Cisco Certified Multi-Multi-Multi-Multi-Edge Partner", "Cisco Certified Multi-Multi-Multi-Multi-Core Partner", "Cisco Certified Multi-Multi-Multi-Multi-Brain Partner", "Cisco Certified Multi-Multi-Multi-Multi-Sense Partner", "Cisco Certified Multi-Multi-Multi-Multi-Act Partner", "Cisco Certified Multi-Multi-Multi-Multi-Think Partner", "Cisco Certified Multi-Multi-Multi-Multi-Feel Partner", "Cisco Certified Multi-Multi-Multi-Multi-Taste Partner", "Cisco Certified Multi-Multi-Multi-Multi-Smell Partner", "Cisco Certified Multi-Multi-Multi-Multi-Touch Partner", "Cisco Certified Multi-Multi-Multi-Multi-Move Partner", "Cisco Certified Multi-Multi-Multi-Multi-Speak Partner", "Cisco Certified Multi-Multi-Multi-Multi-Interact Partner", "Cisco Certified Multi-Multi-Multi-Multi-Engage Partner", "Cisco Certified Multi-Multi-Multi-Multi-Connect Partner", "Cisco Certified Multi-Multi-Multi-Multi-Share Partner", "Cisco Certified Multi-Multi-Multi-Multi-Collaborate Partner", "Cisco Certified Multi-Multi-Multi-Multi-Work Partner", "Cisco Certified Multi-Multi-Multi-Multi-Learn Partner", "Cisco Certified Multi-Multi-Multi-Multi-Grow Partner", "Cisco Certified Multi-Multi-Multi-Multi-Innovate Partner", "Cisco Certified Multi-Multi-Multi-Multi-Transform Partner", "Cisco Certified Multi-Multi-Multi-Multi-Improve Partner", "Cisco Certified Multi-Multi-Multi-Multi-Optimize Partner", "Cisco Certified Multi-Multi-Multi-Multi-Maximize Partner", "Cisco Certified Multi-Multi-Multi-Multi-Amplify Partner", "Cisco Certified Multi-Multi-Multi-Multi-Magnify Partner", "Cisco Certified Multi-Multi-Multi-Multi-Expand Partner", "Cisco Certified Multi-Multi-Multi-Multi-Stretch Partner", "Cisco Certified Multi-Multi-Multi-Multi-Extend Partner", "Cisco Certified Multi-Multi-Multi-Multi-Reach Partner", "Cisco Certified Multi-Multi-Multi-Multi-Access Partner", "Cisco Certified Multi-Multi-Multi-Multi-Reachable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Accessible Partner", "Cisco Certified Multi-Multi-Multi-Multi-Usable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Operable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Manageable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Maintainable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Upgradeable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Replaceable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Disposable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Reusable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Restorable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Recoverable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Resilient Partner", "Cisco Certified Multi-Multi-Multi-Multi-Tolerant Partner", "Cisco Certified Multi-Multi-Multi-Multi-Adaptable Partner", "Cisco Certified Multi-Multi-Multi-Multi-Flexible Partner", "Cisco Certified Multi-Multi-Multi-Multi-Versatile Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multifunctional Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Purpose Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Function Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Feature Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Service Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Application Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-System Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Infrastructure Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Network Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Cloud Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-On-Premise Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Hybrid Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Edge Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Core Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Brain Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Sense Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Act Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Think Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Feel Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Taste Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Smell Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Touch Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Move Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Speak Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Interact Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Engage Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Connect Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Share Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Collaborate Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi-Work Partner", "Cisco Certified Multi-Multi-Multi-Multi-Multi

[see vSphere Hardening Guide]

The Private Cloud Way

- 
1. Expose your interface
 2. Throw a party to celebrate!

Blackberry strikes back

Last year this guy was managing his XEN farm using a bugged Web Interface with his Blackberry



Kyle Bassman

Posts: 167

Re: XenCenterWeb?

Posted: Jul 29, 2009 11:08 AM

 in response to: [Christopher Ca...](#)

 Reply

 0 users found this post useful

I noticed it was gone as well. You all should correct the security flaws and re-release it. Its an awesome interface, and I can admin my Xen Farm from my Blackberry.

Now the Blackberry is back on Xen Cloud Platform!

critical for me. This means that I have to be able to do most if not all of my admin work from my BlackBerry smartphone. That's the beauty of open source, different focus brings different results.

Whatever anyone feels about it, I won't apologize for writing it because someone has written something similar.

Vern

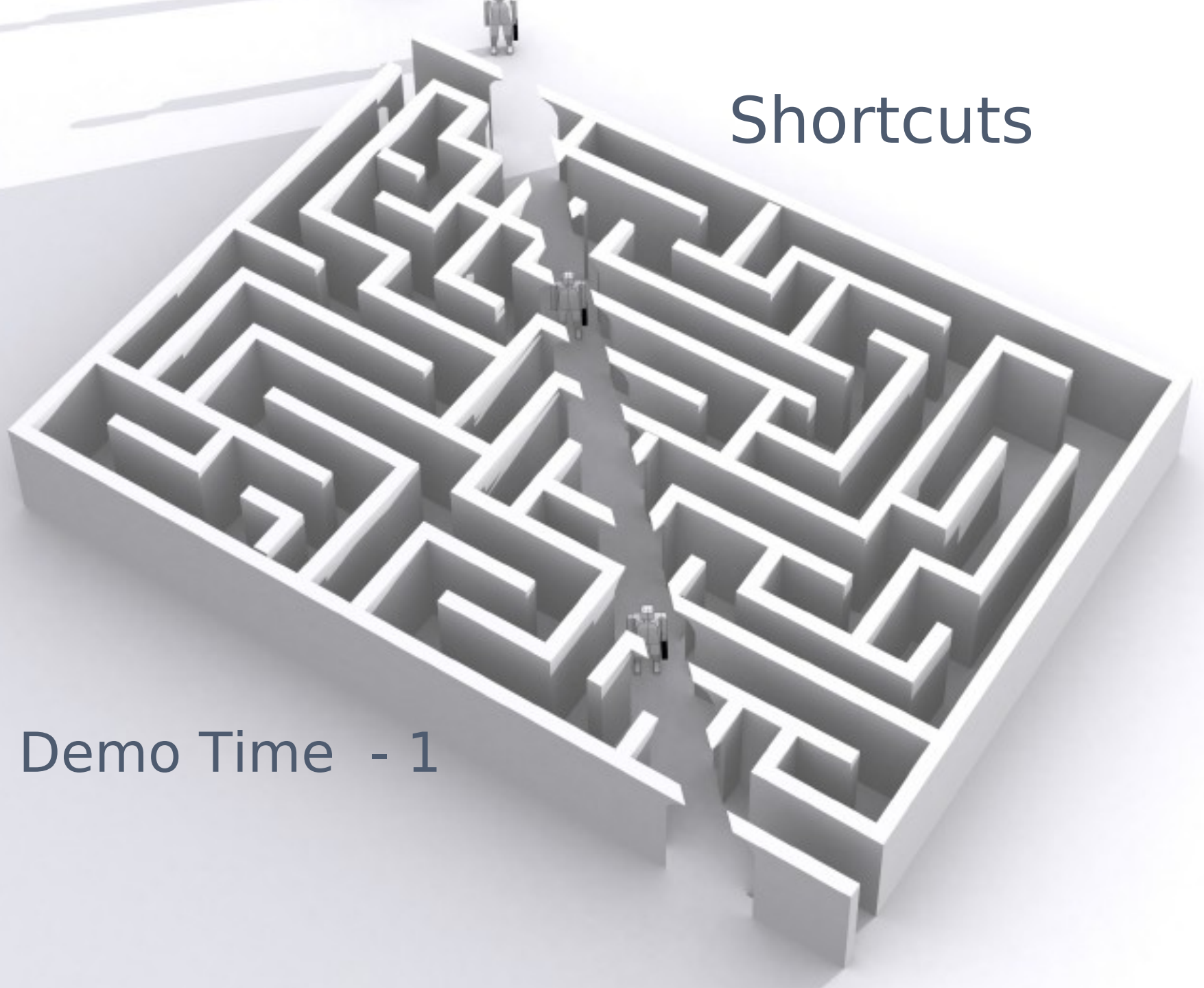
By the way... introducing VASTO

The Virtualization ASsessment TOolkit

It is an “exploit pack” for **Metasploit** focusing on virtualization security.

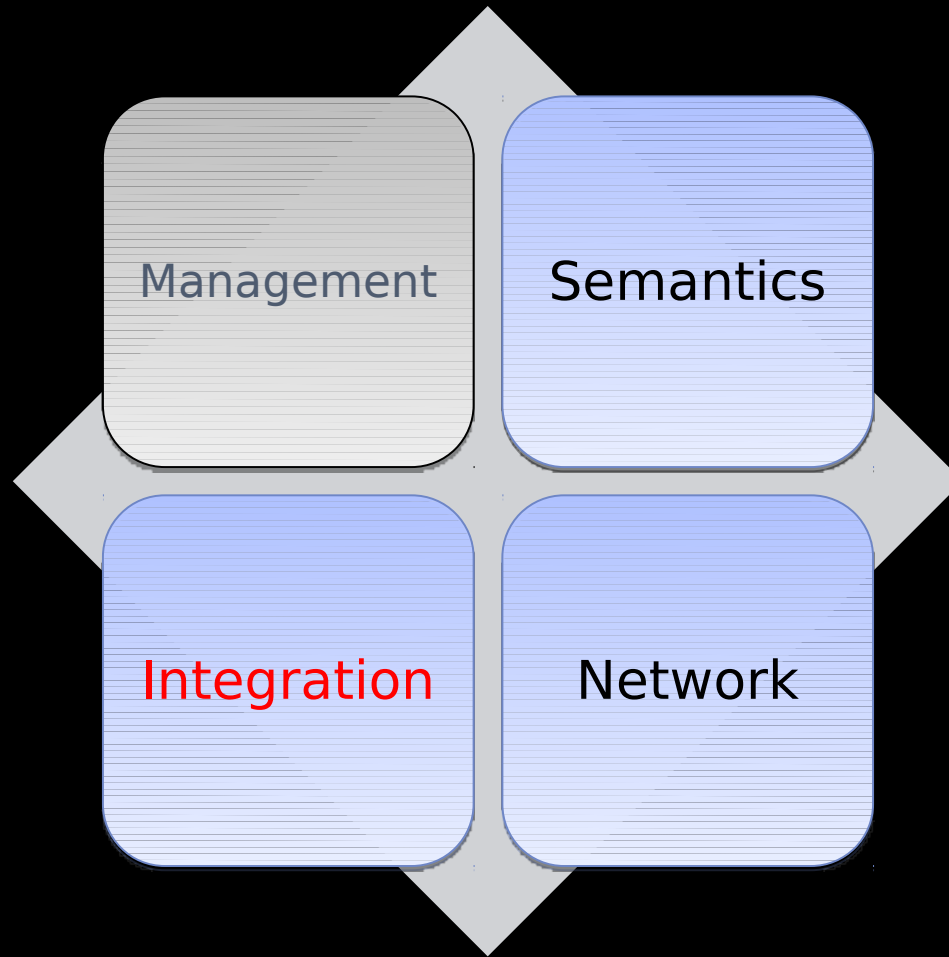
Announcing Beta 0.2 SyScan10 Edition
VASTO now knows some cloud tricks

Shortcuts

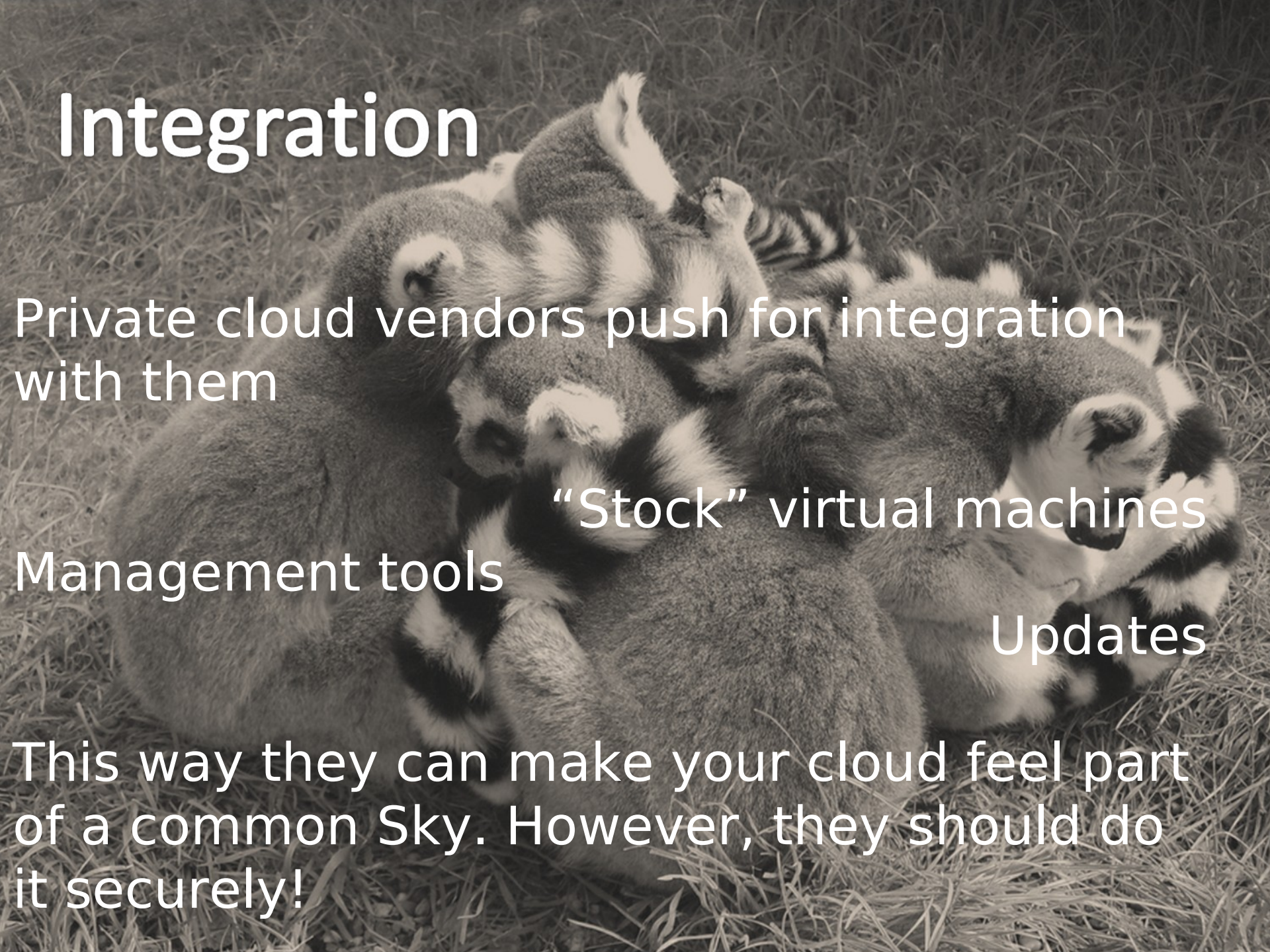


Demo Time - 1

Security Deltas



Integration

A group of lemurs, possibly ring-tailed lemurs, are huddled together in a pile on a bed of dry grass. They are facing various directions, with some looking towards the camera and others looking away. The lemurs have greyish-brown fur with white markings on their faces and chests. Their long, striped tails are visible, some curled up and others extending outwards. The overall scene conveys a sense of unity and integration.

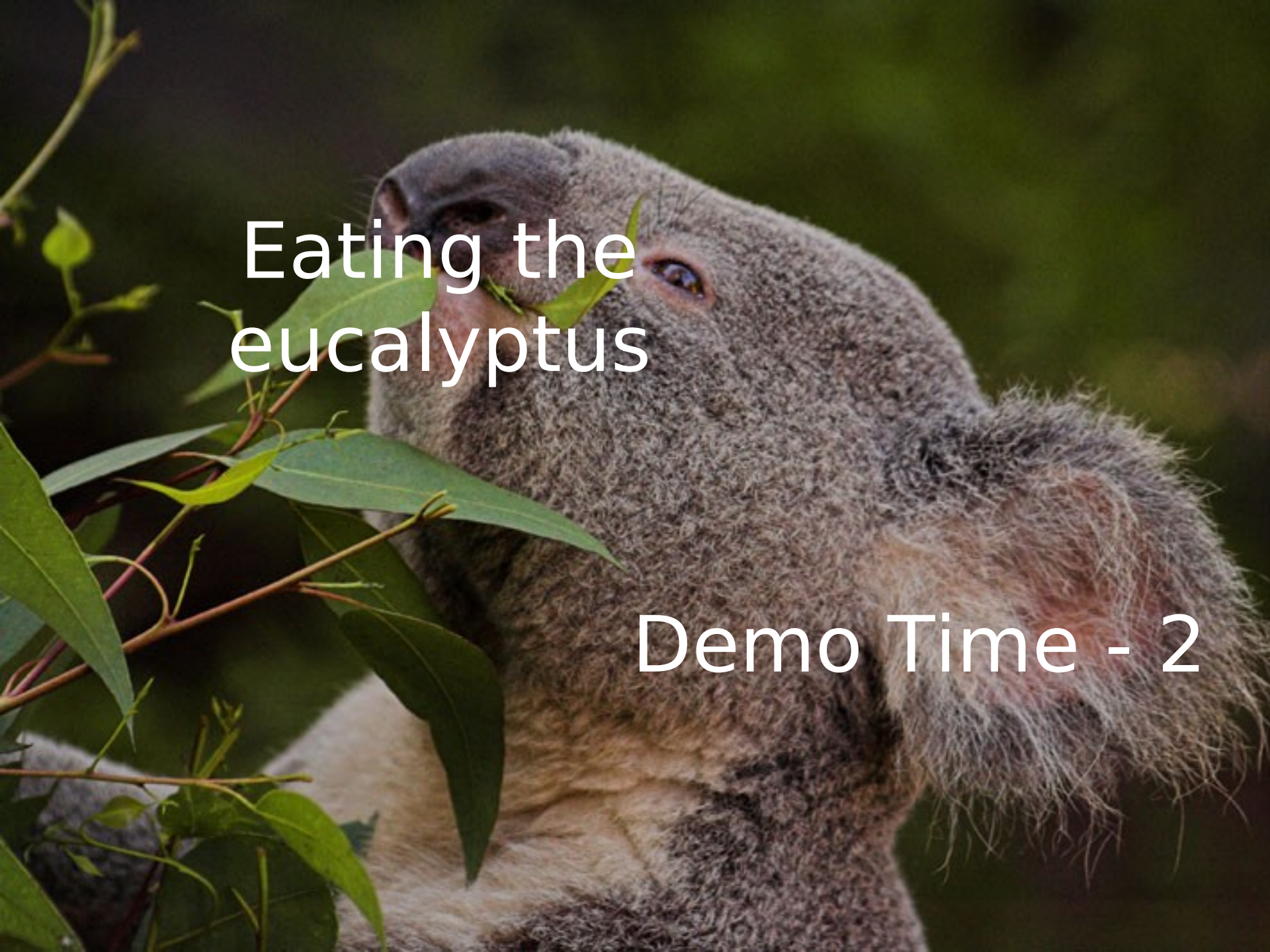
Private cloud vendors push for integration with them

“Stock” virtual machines

Management tools

Updates

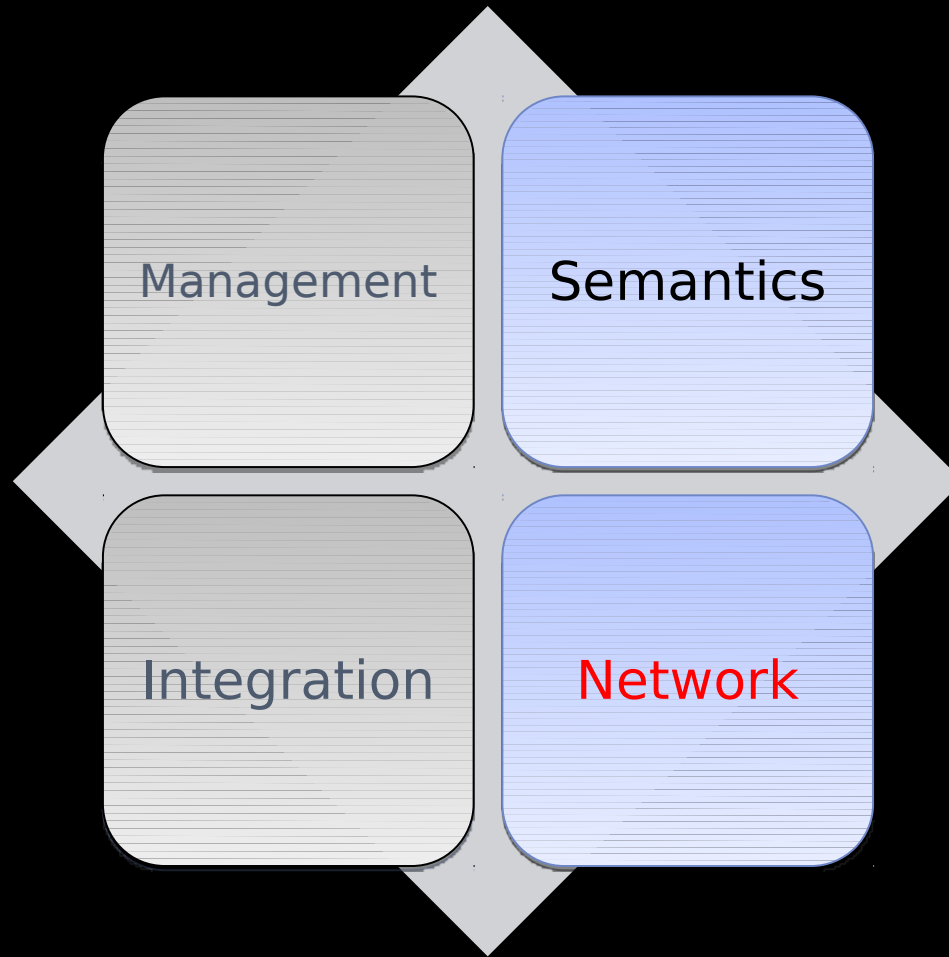
This way they can make your cloud feel part of a common Sky. However, they should do it securely!

A close-up photograph of a koala's head and shoulders. The koala is covered in thick, grey, woolly fur. It is holding a green eucalyptus leaf in its mouth and appears to be eating it. The background is a soft, out-of-focus green, suggesting a forest environment. The lighting is natural, highlighting the texture of the koala's fur and the vibrant green of the leaves.

Eating the
eucalyptus

Demo Time - 2

Security Deltas



Network

New challenges and old issues

VM Migration

- Even between clouds!

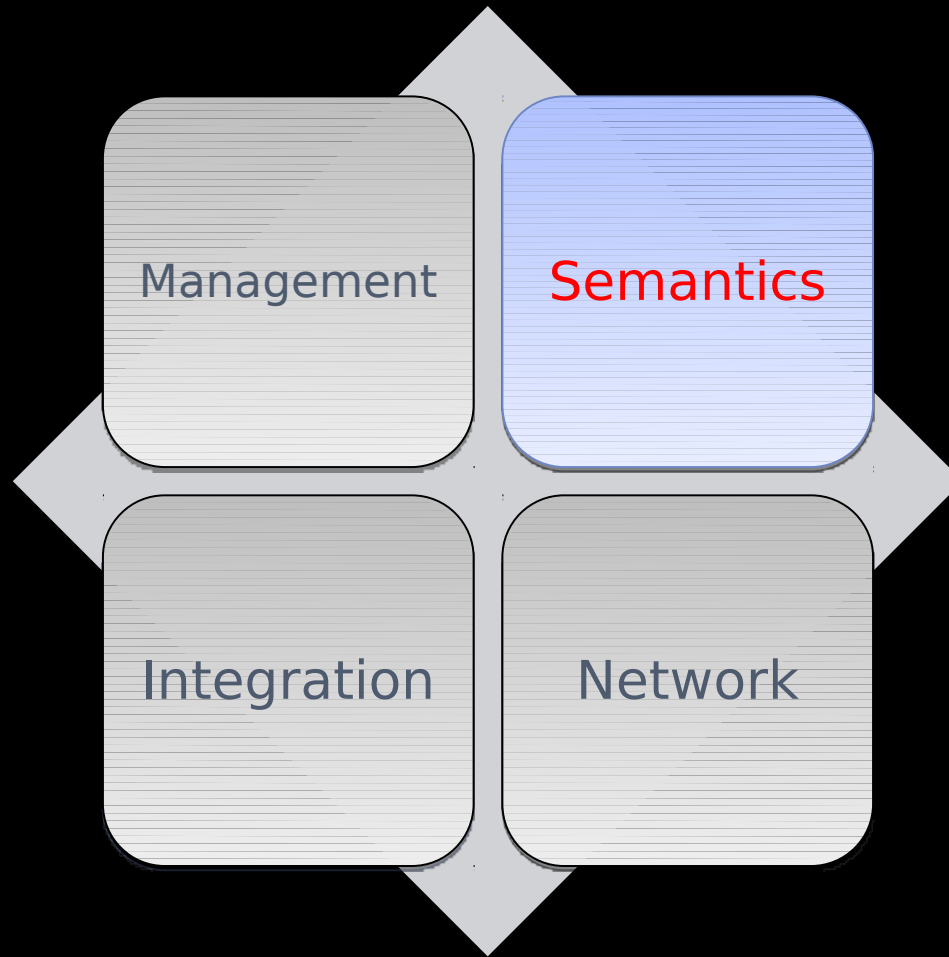
- Still in clear text for most...

Multi tenancy

- Requires (working) network fencing

The whole network stack is a shoot in the dark...

Security Deltas



Semantic of the cloud

The Holy Roman Emperor Charles V was once asked which languages he typically used.

"I speak Spanish to God," he explained, "Italian to women, French to men - and German to my horse."

If you want to make it happen, you have to be able to state that

what-the-cloud-understands = what-the-cloud-can-do

Cloud Paradigm

Thou shall not bypass the interface.

Security labeling

We know that “escape from the VM attacks” will happen again

To mitigate, we can define “zones”

Even if virtualization solutions won't let us do “host tagging”, admins can do it anyway.

Not with Private cloud computing!

A possible solution

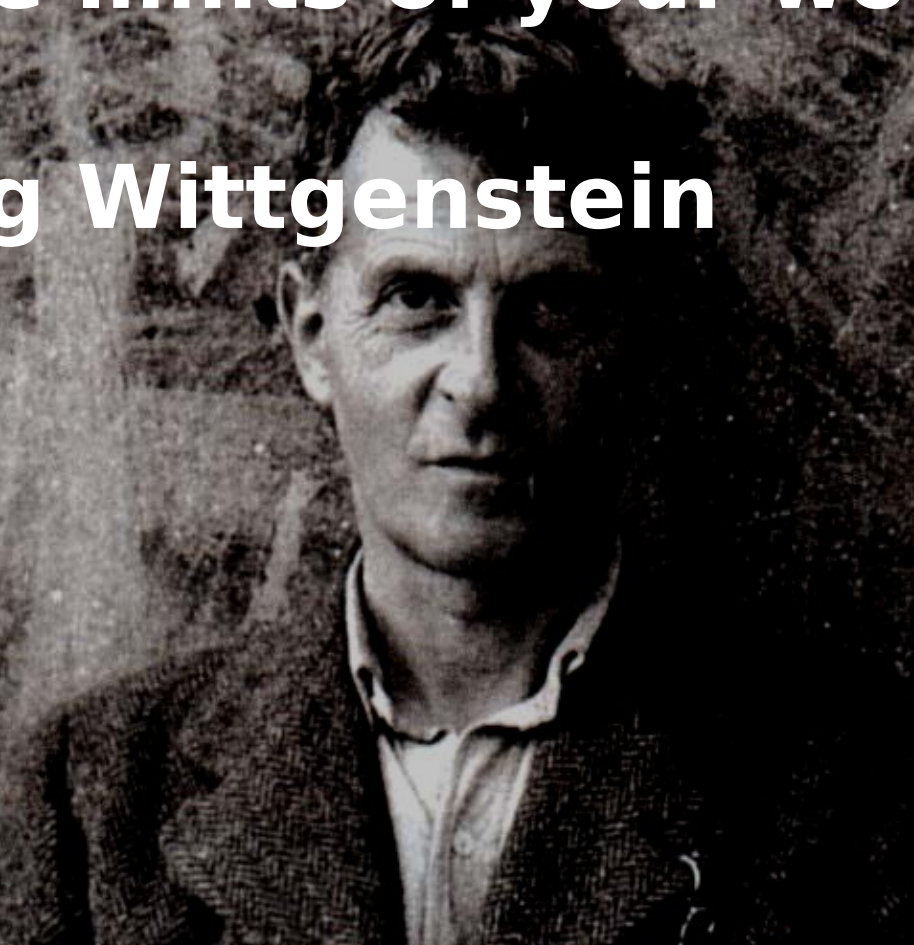
Stating Security Requirements

Who has it, who has not

Cloud Solution	Version tested	Result
Eucalyptus	1.6.2	None
DeltaCloud Portal	0.1.1	Could be
RHEV	NA – Public APIs	None
Abiquo	1.5	None
XEN Cloud Platform	0.1.1	None
Amazon Virtual Private Cloud	NA – March	None (redundancy)
VMware vCloud Express	NA – March	None
Svirt-LibVirt	Library source	Partial
OpenNebula [Haizea]	1.0	Could be

**“ The limits of your language
are the limits of your world ”**

- Ludwig Wittgenstein



Time to make a stand

As “the security community” it’s our role to make sure that new technologies are not simply taken for granted without a security debate.

Private Cloud is a great risk and a great opportunity

We need to make our voice heard!

One more hack

**Off-Premise solutions have to
provide**

Trust and Security

DO THEY?

They're not running in debug mode, are they?

AttributeError at /[REDACTED]/reports/

'NoneType' object has no attribute 'has_key'

Request Method: POST

Request URL: https://[REDACTED]/reports/

Exception Type: AttributeError

Exception Value: 'NoneType' object has no attribute 'has_key'

Exception Location: /usr/local/vmware/labCloud/lib/labCloud/[REDACTED]views.py in listReports, line 1237

Python Executable: /usr/bin/python

Python Version: 2.6.2

Python Path: ['/usr/local/lib/python2.6/dist-packages/ZSI-2.1_a1-py2.6.egg', '/usr/local/lib/python2.6/dist-packages/pycha-0.5.2-py2.6.egg', '/usr/local/lib/python2.6/dist-packages/python_daemon-1.5.2-py2.6.egg', '/usr/local/lib/python2.6/dist-packages/lockfile-0.8-py2.6.egg', '/usr/local/lib/python2.6/dist-packages/python_memcached-1.45-py2.6.egg', '/usr/local/lib/python2.6/dist-packages/PyRRD-0.0.7-py2.6.egg', '/usr/local/lib/python2.6/dist-packages/M2Crypto-0.20.2-py2.6-linux-i686.egg', '/usr/lib/python2.6', '/usr/lib/python2.6/plat-linux2', '/usr/lib/python2.6/lib-dynload', '/usr/local/lib/python2.6/dist-packages', '/var/lib/python-support/python2.6', '/var/lib/python-support/python2.6/gtk-2.0', '/usr/local/lib/python2.6/dist-packages', '/usr/local/vmware/labCloud/lib/labCloud', '/usr/local/vmware/labCloud/lib', '/usr/local/vmware/labCloud/lib/labCloud']

Server time: [REDACTED] 2010 [REDACTED]

Traceback [Switch to copy-and-paste view](#)

/usr/local/lib/python2.6/dist-packages/django/core/handlers/base.py in get_response

92. response = callback(request, *callback_args, **callback_kwargs)

► Local vars

/usr/local/vmware/labCloud/lib/labCloud/auth/decorators.py in __call__

79. return self.view_func(request, *args, **kwargs)

► Local vars

/usr/local/vmware/labCloud/lib/labCloud/[REDACTED]views.py in listReports

1237. if detailedReport.has_key("actionResult") and detailedReport["actionResult"] != "SUCCESS":

► Local vars

Hate the Sin not the Sinner

What is everyone doing?

HTTP/1.1 200 OK

Server: Apache/2.2.14 (Unix) mod_ssl/2.2.14 OpenSSL/0.9.8g
mod_wsgi/2.6 Python/2.6.2

Vary: Accept-Language, Cookie, Accept-Encoding

Expires: -1

Content-Language: en

Pragma: no-cache

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Content-Length: 114

```
[["0", ["7810", "$ANYUSERNAME", "COMPLETED", "updateThumbs",  
"Task completed successfully", "2010/03/22 17:03:35"]]]
```

Hate the Sin not the Sinner

(re)Think about your Cloud strategy

You need one!

Check security of outsourcer

Make your voice heard!

Questions



A person is silhouetted against a bright sunset, standing on a dark, rocky mountain peak. The sun is a large, glowing orb in the center of the frame, casting a warm orange and yellow light across the sky. Below the sun, a vast, undulating sea of white and orange-tinted clouds stretches to the horizon. The person's arm is raised, and they appear to be looking through binoculars or a telescope at the horizon.

Standing on the Clouds

Claudio Criscione
c.criscione@securenetwork.it
Twitter @paradoxengine
VASTO's home is at nibblesec.org